REMARKS

Claims 1-10 are pending in the Application.

Claims 1-10 stand rejected.

Claims 1, 4, 7-8 and 10 stand rejected under 35 U.S.C. § 103 as being unpatentable over *Mattison* (U.S. Patent No. 6,363,463), in view of *Grawrock* ("Building Trust and Privacy Into Open PC Systems," November 2000). In response, Applicants respectfully traverse these rejections.

Mattison updates a flash memory program with an upgrade, using a new flash memory image after verifying the source and content of the flash memory upgrade program using a digital signature. Column 3, lines 25-60. With this scheme, only the holders of the vendor's private key could distribute software to modify the program. Column 4, lines 28-30. The Examiner admits that *Mattison* does not teach using a trusted platform module (TPM).

The Examiner asserts that *Grawrock* teaches a TPM to perform the authorization of a BIOS boot loader to a digital signature technique. The Examiner then goes on to assert that it would have been obvious to combine *Grawrock* and *Mattison* to arrive at the claimed invention. Applicants respectfully disagree.

The Examiner is respectfully requested to refer to the declaration under 37 C.F.R. §1.132 (the "132 Declaration") by the inventors who have reviewed the prior art. According to the inventors, *Grawrock* teaches that the verification of the BIOS occurs after it has already been loaded onto the system. The present invention verifies the authenticity of the BIOS before allowing it to be stored on the flash memory of the system. The difference between these two processes is like the difference between catching a criminal after the crime has been committed versus preventing the crime.

The claims specifically recite that the memory unit is unlocked after the verification is successful. According to the inventors, *Grawrock* already stores the updated program, and then performs a TPM verification. Thus, the prior art teaches away from the present invention.

Furthermore, the Examiner has not in anyway addressed this claim limitation in this rejection. Further, in the rejection below, the Examiner adds in the *Hale* reference in order to address this limitation. Thus, the Examiner's *prima facie* case is insufficient.

Claims 2-3, 5-6 and 9 stand rejected under 35 U.S.C. § 103 as being unpatentable over *Mattison* in view of *Grawrock*, and in view of *Hale* (U.S. Patent No. 6,564,371). In response, Applicants respectfully traverse these rejections.
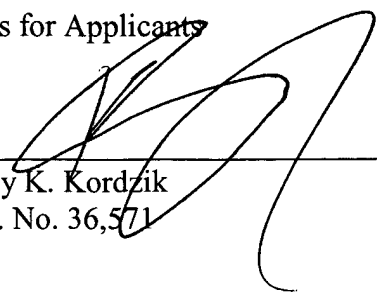
First, the arguments presented above are applicable with respect to these rejections also. Furthermore, the 132 Declaration is also respectfully referred to by the Examiner to show that one skilled in the art at the time the invention was made would not have combined the three references in the manner as suggested by the Examiner. The inventors declare that the image must first be authorized as being authentic by the TPM before the TPM will unlock the flash memory unit. The present invention differs in that authentication of the image can occur after the unlocking of the flash unit, which can be done more easily than if the TPM is in charge of locking and unlocking the flash unit, as in accordance with the present invention. If one were to combine the three prior art references at the time of filing of the present invention, the result would have been a system where authentication of the image is done after it has been stored on the memory unit after unlocking the memory unit. The present invention as claimed recites a TPM verification performed to determine whether to unlock the memory unit, along with a verification of the image by the TPM also.

As a result of the foregoing, Applicants respectfully assert that the claims are not obvious in view of the prior art.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Applicants

By:_____

    Kelly K. Kordzik

    Reg. No. 36,571

P.O. Box 50784

Dallas, Texas 75201

(512) 370-2851

Austin_1\256516\1

7036-P177US 2/14/2005